REMARKS/ARGUMENTS

Applicant respectfully requests reconsideration of this application in view of the following remarks.

Applicant has amended claims 1, 14, 17, and 22. No new matter has been added. Support for the amendments may be found in the claims, the detailed description, and the figures as originally submitted.

Claim 1 Rejection under 35 U.S.C. § 102(e) - Crump

As amended Applicant's claim 1 recites:

1. (currently amended) A method for traversing a firewall, comprising:

initiating a first connection to go through said firewall;

evaluating the first connection for a response from a remote system indicating a successful first connection;

initiating a second connection to go through said firewall if a successful first connection is not established;

evaluating the second connection for a response from a remote system indicating a successful second connection;

initiating a third connection to go through said firewall if a successful second connection is not established; and

evaluating the third connection for a response from a remote system indicating a successful third connection.

[Emphases added.]

The Office cites on page 3 paragraph 4 Crump at column 4, lines 5-33 as anticipating Applicant's claim 1. For a reference to anticipate a claim each and every element of the claim must be exactly disclosed in the anticipatory reference. Applicant submits that as amended, Crump does not disclose initiating connections to go through a firewall as in Applicant's as amended claim 1. Additionally, nowhere does Crump even mention a firewall. As such, Crump does not anticipate Applicant's claim1. Applicant respectfully requests removal of this rejection for claim 1 and for claims dependent on claim 1 specifically claims 2, 3, 4, 10, and 12 which were also rejected under 102(e).

Claim 4 Rejection under 35 U.S.C. § 103(a) - Crump in view of Bhide

Applicant's claim 4 recites:

4. (original) The method according to claim 2, wherein initiating a HTTP connection comprises initiating a HTTP connection to a predefined address using port 80.

Applicant's claim 4 is dependent on claim 2, which is in turn dependent on claim 1. The issue of a 102(e) Crump rejection for claims 1, and 2 are addressed above and incorporated herein.

The Office (page 5, paragraph 7) cites Bhide for "Bhide et al teaches initiating a HTTP connection that comprises initiating a HTTP connection to a predefined address using port 80 [column 5, lines 9-21]."

Applicant submits that modifying Crump so that a HTTP connection using port 80 is used still does not yield Applicant's claim 4 because as explained above it does not disclose or suggest a firewall as in Applicant's amended claim 1. Nor does Bhide disclose or even mention a firewall. Combining Bhide with Crump does not cure this and therefore Crump in view of Bhide does not make obvious what Applicant has claimed in claim 4. Applicant therefore respectfully requests removal of this rejection for claim 4.

Claims 5-9 Rejection under 35 U.S.C. § 103(a) - Crump in view of Fuh

The Office (page 6, paragraph 8) cites Fuh for:

Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port [column 13, lines 3-14]. **[Claim 5]**

Fuh et al teaches that determining a likely proxy address and port further comprises packet sniffing [column 9, lines 51-67]. **[Claim 6]**

Fuh et al teaches that packet sniffing further comprises: sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports [column 9, lines 51-67]. **[Claim 7]**

Fuh et al teaches that extracting information from the sampled packets comprises examining TCP packets for HTTP data [column 9, lines 51-67]. **[Claim 8, and 9]**

[Bracketed bolded added for ease of discussion]

Specifically with respect to claim 5

Applicant's claim 5 recites:

5. (original) The method according to claim 2, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port.

[Emphasis added.]

Applicant's claim 5 is dependent on claim 2, which is in turn dependent on claim 1. The issue of a 102(e) Crump rejection for claims 1, and 2 are addressed above and incorporated herein.

Applicant submits that Fuh is fundamentally different than Applicant's claim 5. While Applicant teaches determining a likely proxy address and port, Fuh (see Abstract) on the other hand teaches "network access control" and "intercept network traffic." Further, Fuh Figure 2 at 210 clearly shows intercepting traffic to/from 206 and 216 and the specification details authentication based on AA server 218 and Database 220. Network access control and intercepting network traffic (Fuh) is not the same as determining a likely proxy address and port (Applicant's claim 5)

Additionally, while the Office states "Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address and port [column 13, lines 3-14]." Applicant submits that the cited lines discuss the authentication process and do not teach anything about determining a like proxy address and port as in Applicant's claim 5.

Finally, modifying Crump with Fuh does not disclose or make obvious the "firewall" aspect of claim 1 or the "determining a likely proxy address and port" aspect of claim 5. Applicant respectfully requests removal of this rejection for claim 5 and claims 6-9 which are dependent on claim 5.

Specifically with respect to claim 6

Applicant's claim 6 recites:

6. (original) The method according to claim 5, wherein determining a likely proxy address and port further comprises packet sniffing.

[Emphasis added.]

The Office cites Fuh for "Fuh et al teaches that determining a likely proxy address and port further comprises packet sniffing [column 9, lines 51-67]."

Applicant submits that Fuh actually teaches away from Applicant's claim 6. While Applicant teaches sniffing packets which does not involve altering in any way the communication, Fuh (see Abstract) on the other hand teaches network access control and intercepting network traffic. Intercepting network traffic (Fuh) is the *antithesis* of packet sniffing (Applicant).

Further, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address and port further comprises packet sniffing as in Applicant's claim 6. Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Finally, modifying Crump with Fuh does not disclose or make obvious the "packet sniffing" aspect of claim 6. Applicant respectfully requests removal of this rejection for claim 6 and claims 7-9 which are dependent on claim 6.

Specifically with respect to claim 7

Applicant's claim 7 recites:

7. (original) The method according to claim 6, wherein packet sniffing further comprises:

sampling packets;

extracting information from the sampled packets; and

building a database of likely proxy addresses and ports.

The Office cites Fuh for "Fuh et al teaches that packet sniffing further comprises: sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports [column 9, lines 51-67]."

Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports as in Applicant's claim 7.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

As discussed above for claim 6, Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Finally, modifying Crump with Fuh does not disclose or make obvious the "sampling packets; extracting information from the sampled packets; and building a database of likely proxy addresses and ports" aspect of claim 7. Applicant respectfully requests removal of this rejection for claim 7 and claims 8-9 which are dependent on claim 7.

Claims 11 and 13 Rejection under 35 U.S.C. § 103(a) - Crump in view of Fuh

The Office (page 7, paragraph 9) cites Fuh for: "Fuh et al teaches initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting IP and Ethernet addresses [column 9, lines 51-67]."

Specifically with respect to claim 11

Applicant's claim 11 recites:

11. (original) The method according to claim 10, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting IP addresses.

As detailed above, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sampling packets and extracting IP addresses as in Applicant's claim 11. Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Filtering packets and not forwarding packets (Fuh) is not the same as sampling packets or extracting IP addresses (as in Applicant's claim 11).

Finally, modifying Crump with Fuh does not disclose or make obvious the "determining a likely proxy address by sampling packets and extracting IP addresses" aspect of claim 11. Applicant respectfully requests removal of this rejection for claim 11.

Specifically with respect to claim 13

Applicant's claim 13 recites:

13. (original) The method according to claim 12, wherein initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sampling packets and extracting Ethernet addresses.

As detailed above, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sampling packets and extracting Ethernet addresses as in Applicant's claim 13. Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Filtering packets and not forwarding packets (Fuh) is not the same as sampling packets or extracting Ethernet addresses (as in Applicant's claim 13).

Finally, modifying Crump with Fuh does not disclose or make obvious the "determining a likely proxy address by sampling packets and extracting Ethernet addresses" aspect of claim 13. Applicant respectfully requests removal of this rejection for claim 13.

Claim 14 Rejection under 35 U.S.C. § 102(e) - Crump

As amended Applicant's claim 14 recites:

14. (currently amended) A machine-readable medium having stored thereon instructions, which when executed by a processor, causes said processor to perform the following:

initiate a first connection to go through a firewall;

evaluate the first connection for a response from a remote system indicating a successful first connection;

initiate a second connection to go through said firewall if a successful first connection is not established;

evaluate the second connection for a response from a remote system indicating a successful second connection;

initiate a third connection to go through said firewall if a successful second connection is not established; and

evaluate the third connection for a response from a remote system indicating a successful third connection.

As discussed above in claim 1, the Office cites on page 3 paragraph 4 Crump at column 4, lines 5-33 as anticipating Applicant's claim 14. For a reference to anticipate a claim each and every element of the claim must be exactly disclosed in the anticipatory reference. Applicant submits that as amended, Crump does not disclose initiating connections to go through a firewall as in Applicant's as amended claim 14. Additionally, nowhere does Crump even mention a firewall. As such, Crump does not anticipate Applicant's claim14. Applicant respectfully requests removal of this rejection for claim 14 and for claims dependent on claim 14.

Claim 16 Rejection under 35 U.S.C. § 103(a) - Crump in view of Linden

Applicant's claim 16 recites:

16. (original) The machine-readable medium according to claim 15, further configuring said processor to perform the following:

examine network traffic; and

build a database of parameters likely to allow establishment of a HTTP connection via a proxy connection.

Firstly, the Office (page 8, paragraph 10) states: "As to claim 16, Crump et al teaches examining network traffic [column 5, lines 47-67].

Applicant submits that the cited lines discuss the translating apparatus and do not teach anything about examining network traffic as in Applicant's claim 16.

Specifically Crump discloses:

In order for the X.25 devices 102 to communicate with the TCP device … it is necessary for end-to-end connections to be established between the X.25 devices 102 and the TCP device 118. …there must be both an active X.25 connection … and the translating apparatus 110 and an active TCP connection… X.25 devices 102 communicate with the translating apparatus … the TCP device 118 communicates with the translating apparatus 110….

Crump does not disclose examining network traffic nor does the combination with Linden cure this. Applicant respectfully requests removal of this rejection for claim 16.

Secondly, the Office (page 8, paragraph 10) states: "Linden et al teaches building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection [column 5, lines 16-26]."

Applicant submits that the cited lines discuss protocols and do not teach anything about building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection as in Applicant's claim 16.

Specifically the cited lines state:

A particular advantage of the invention e.g. in connection with the WAP application protocol is that it is possible to efficiently utilize functions connected with the HTTP data transmission protocol of the WSP/B protocol already known as such. These include, for example, GET, PUT, and POST requests. Consequently, the header fields of the HTTP protocol can also be utilized in the data transmission, as well as the headers of the HTTP protocol for authentication. Correspondingly, it is possible to utilize efficiently the methods of the WWW communication network for authorization or data transmission.

Applicant submits that there is nothing in the cited section that even remotely suggests building a database of parameters likely to allow establishment of a HTTP connection via a proxy connection as in Applicant's claim 16.

Crump in view of Linden does not make obvious what is in Applicant's claim 16. Applicant therefore respectfully requests removal of this rejection for claim 16.

Claim 17 Rejection under 35 U.S.C. § 102(e) - Crump

As amended Applicant's claim 17 recites:

17. (currently amended) A firewall traversal system comprising:

a main system coupled to storage;

a communication subsystem coupled to the main system and a communication medium on one side of a firewall;

a packet examining subsystem coupled to the communication subsystem; and

a database system coupled to the packet examining subsystem and the main system.

[Emphasis added.]

The Office cites on page 4, paragraph 6 Qu as anticipating Applicant's claim 17. For a reference to anticipate a claim each and every element of the claim must be exactly disclosed in the anticipatory reference. Applicant submits that as amended, Qu does not disclose a communication medium on one side of a firewall as in Applicant's as amended claim 17. Qu specifically teaches (see Title) "firewall processing." Qu figure 3 clearly shows processing within the firewall 40. As such, Qu does not anticipate Applicant's claim 17 element of "a communication subsystem coupled to the main system and a communication medium on one side of a firewall." Applicant therefore respectfully requests removal of this rejection for claim 17 and for all claims dependent on claim 17.

Claims 22-26 Rejection under 35 U.S.C. § 102(e) - Crump

As amended Applicant's claim 22 recites:

22. (currently amended) A method for traversing a firewall, comprising:

means for initiating a first connection to go through said firewall;

means for evaluating the first connection for a response from a remote system indicating a successful first connection;

means for initiating a second connection to go through said firewall if a successful first connection is not established;

means for evaluating the second connection for a response from a remote system indicating a successful second connection;

means for initiating a third connection to go through said firewall if a successful second connection is not established; and

means for evaluating the third connection for a response from a remote system indicating a successful third connection.

[Emphases added.]

As discussed above with respect to claim 1, the Office cites on page 3 paragraph 4 Crump at column 4, lines 5-33 as anticipating Applicant's claim 22. For a reference to anticipate a claim each and every element of the claim must be exactly disclosed in the anticipatory reference. Applicant submits that as amended, Crump does not disclose initiating connections to go through a firewall as in Applicant's as amended claim 22. Additionally, nowhere does Crump even mention a firewall. As such, Crump does not anticipate Applicant's claim 22. Applicant respectfully requests removal of this rejection for claim 22 and for all claims dependent on claim 22.

Claims 24 and 25 Rejection under 35 U.S.C. § 103(a) - Crump in view of Fuh

Specifically with respect to claim 24

Applicant's claim 24 recites:

24. (original) The apparatus of claim 23, wherein means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sniffing packets and extracting information from the packets.

[Emphasis added.]

The Office (page 9, paragraph 11) states:

> Fuh teaches means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by sniffing packets and extracting information from the packets [column 9, lines 51-67].

Applicant submits that Fuh actually teaches away from Applicant's claim 24. While Applicant teaches sniffing packets which does not involve altering in any way the communication, Fuh (see Abstract) on the other hand teaches network access control and intercepting network traffic. Intercepting network traffic (Fuh) is the *antithesis* of packet sniffing (Applicant).

Further, Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by sniffing packets and extracting information from the packets as in Applicant's claim 24.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input

ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Fuh teaches away from packet sniffing and deals with filtering packets, not forwarding packets, and controlling delivery.

Finally, modifying Crump with Fuh does not disclose or make obvious the "packet sniffing" aspect of claim 24. Applicant respectfully requests removal of this rejection for claim 24.

Specifically with respect to claim 25

Applicant's claim 25 recites:

25. (original) The apparatus of claim 23, wherein means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall.

[Emphasis added.]

The Office (page 9, paragraph 11) states:

Fuh teaches means for initiating a HTTP connection via a proxy connection further comprises determining a likely proxy address by receiving information from a computer connected to the firewall [column 9, lines 51-67].

Applicant submits that the cited lines discuss the Authentication and Authorization process and do not teach anything about determining a likely proxy address by receiving information from a computer connected to the firewall as in Applicant's claim 25.

Fuh at the lines cited specifically says "Access control lists filter packets .... If the IP address of client 306 is not stored in input ACL 424, then firewall router 210 will not forward the packet further within the circuitry or software of the firewall router. Output ACL 426 similarly controls the delivery of packets from firewall router 210 to resources located outside external interface 420."

[Emphases added.]

Finally, modifying Crump with Fuh does not disclose or make obvious the "receiving information from a computer connected to the firewall" aspect of claim 25. Applicant respectfully requests removal of this rejection for claim 25.

Claim 26 Rejection under 35 U.S.C. § 103(a) - Crump in view of Montenegro

Applicant's claim 26 recites:

26. (original) The apparatus of claim 22, further comprising means for updating firewall traversal strategies.

[Emphasis added.]

The Office (page 10, paragraph 12) states "Montenegro teaches means for updating firewall traversal strategies [column 6, lines 49-65]."

[Emphasis added.]

Applicant submits that the cited lines discuss obtaining a RAFT URL. Obtaining is different than updating. Obtaining does not teach updating as in Applicant's claim 26.

Montenegro at the lines cited specifically says:

> The first step in creating a transparency between the firewall traversal for remote access and the client application is to obtain the appropriate RAFT URL (step 510). The discovery of the specific RAFT URL to use ... may be achieved in several ways: (1) obtaining it in person..., (2)... user may retrieve the appropriate RAFT URL from the firewall, (3) querying a directory service... or (4) may be preconfigured into the client application or system.

Nowhere does Montenegro discuss or disclose updating firewall traversal strategies as in Applicant's claim 26.

Finally, modifying Crump with Montenegro does not disclose or make obvious the "updating firewall traversal strategies" aspect of claim 26. Applicant respectfully requests removal of this rejection for claim 26.

CONCLUSION

Applicant submits that the rejection of dependent claims not specifically addressed, are addressed by Applicant's arguments to the claim(s) on which they depend.

Applicant respectfully submits that all claims are in condition for allowance and requests such.

Communication via cleartext email is authorized.

Respectfully submitted,

Heimlich Law

Alan Heimlich

Digitally signed by Alan Heimlich
DN: CN = Alan Heimlich, C = US, O = Heimlich Law

11/05/2005

Date

Alan Heimlich / Reg 48808

Attorney for Applicant(s)

Customer No. 40418

5952 Dial Way
San Jose, CA 95129

Tel: 408 253-3860
Eml: alanheimlich@heimlichlaw.com